Module-V

The E-COMMERCE Security Environment, Security Threats in The E-COMMERCE Environment, E-COMMERCE Payment Systems.

THE E-COMMERCE SECURITY ENVIRONMENT

1. **Introduction to Cybercrime**: The internet provides opportunities for both law-abiding citizens and criminals. Criminals exploit the internet for various illegal activities, including theft, fraud, and cyberattacks. Cybercrime can be highly lucrative, and the anonymity of the internet makes it less risky for criminals.
2. **Cost of Cybercrime**: Cybercrime has significant financial consequences for both businesses and consumers. The costs include not only the direct losses due to criminal activities but also the expenses associated with securing networks, recovering from cyberattacks, and addressing potential reputational damage. The losses incurred due to cyber fraud activity in India spiked to over 1.7 billion Indian rupees in the financial year 2024.
3. **Estimating Cybercrime**: Estimating the total economic impact of cybercrime is challenging due to underreporting and difficulties in quantifying losses. Various studies and reports attempt to estimate the scale of cybercrime, with estimates ranging from hundreds of billions of dollars globally.
4. **Types of Cyberattacks**: The passage mentions various types of cyber threats, including botnet attacks, DDoS attacks, Trojans, phishing, ransomware, data theft, identity fraud, credit card fraud, and spyware. These threats are constantly evolving and present challenges to e-commerce security.

1. **Online Credit Card Fraud**: Online credit card fraud is highlighted as a significant issue, with criminals increasingly stealing and distributing large numbers of credit card details for criminal purposes.
2. **Underground Economy Marketplace**: Stolen information is valuable to cybercriminals, and they often sell it on underground marketplaces on the dark web. The passage provides examples of prices for various types of stolen data.
3. **Security and E-Commerce**: E-commerce security is multi-layered and requires a combination of technologies, organizational policies, and procedures, as well as industry standards and government laws to protect the interests of both consumers and businesses.

Risks in E-Commerce:

1. E-commerce involves risks similar to traditional commerce, including the loss of privacy, potential theft, and fraud.
2. Risks for consumers include not receiving purchased items or experiencing unauthorized financial transactions.
3. Risks for merchants include non-payment for goods and services or fraudulent payment methods.

Complex Risk Reduction:

1. E-commerce security is a complex process that involves various strategies and measures to mitigate risks.
2. This process encompasses the use of new technologies, organizational policies and procedures, and legal and industry standards.
3. The ultimate goal is to empower law enforcement officials to investigate and prosecute offenders.

Multilayered Security:

1. E-commerce security should be multilayered, as illustrated in Figure 5.1, involving multiple defenses and safeguards to protect against threats.

Technologies and Tools:

1. Various security technologies and tools are available to enhance e-commerce security.
2. These tools should be employed to protect digital transactions, data, and sensitive information.
3. Examples include encryption, firewalls, and intrusion detection systems.

Organizational Policies:

1. It's essential for organizations to establish and enforce security policies and procedures.
2. These policies ensure that security technologies are effectively implemented and that employees follow best practices.

Legal and Industry Standards:

1. Good e-commerce security involves adhering to relevant laws and industry standards.
2. Legal measures can enforce payment mechanisms and provide a framework for investigating and prosecuting violations of security-related laws.

Security Is Not Absolute:

1. Perfect security is not achievable; instead, the goal is to manage and minimize risks.
2. The level of security should be appropriate to the value and time sensitivity of the information being protected.

Weakest Link:

1. Security is only as strong as its weakest link, and often, human error or lapses in security policies can be the most vulnerable points.
2. Security measures need to consider all aspects of an organization and its processes.

FIGURE 5.1 **THE E-COMMERCE SECURITY ENVIRONMENT**

E-commerce security is multi-layered, and must take into account new technology, policies and procedures, and laws and industry standards.

4. **Dimensions of E-Commerce Security**: Six key dimensions of e-commerce security are mentioned: integrity, nonrepudiation, authenticity, confidentiality, privacy, and availability. E-commerce security aims to protect these dimensions, and when any of them is compromised, security as a whole is affected.

- **Integrity**:
  - Ensures that information transmitted or received over the Internet is not altered by unauthorized parties.
  - Example: Preventing unauthorized changes to online communications or transactions, such as tampering with a bank wire transfer.
- **Nonrepudiation**:
  - Ensures that e-commerce participants cannot deny their online actions.
  - Example: Prevents individuals from making online posts or orders and later denying their involvement, protecting against disputes.
- **Authenticity**:
  - Ensures the ability to verify the identity of individuals or entities in online interactions.
  - Example: Verifying that the website operator is indeed who they claim to be, preventing impersonation or "spoofing."

- **Confidentiality**:
  - Ensures that messages and data are only accessible to authorized individuals.
  - It is different from privacy.
  - Example: Safeguarding sensitive information from unauthorized access, maintaining data confidentiality.
- **Privacy**:
  - Involves controlling the use of customer information provided to e-commerce merchants.
  - E-commerce businesses must establish internal policies to govern the use of customer data and protect it from illegitimate or unauthorized use.
- **Availability**:
  - Ensures that e-commerce sites function as intended and remain accessible.
  - Example: Ensuring that a website remains operational even when facing potential disruptions or cyberattacks.

5. **Tension Between Security and Other Values**: The passage discusses the trade-off between security and ease of use. While enhancing security is essential, excessive security measures can hinder user experience and profitability. There's a balance to be struck.
6. **Public Safety and Criminal Uses of the Internet**: The tension between individual privacy and public safety is highlighted. Governments and law enforcement agencies need to strike a balance between ensuring public safety and respecting individual privacy in the context of digital communication and surveillance.

E-COMMERCE PAYMENT SYSTEMS

1.Online Payment Systems: Online payments have become a significant part of e-commerce, with a market size exceeding $5 trillion in 2020. The primary form of online payment in the United States remains credit and debit cards.

2.Alternative Payment Systems: Alternative payment systems, including mobile wallet apps and services like PayPal, have gained popularity. Mobile wallet apps are the fastest-growing form of alternative payment systems, with around 35% of smartphone users using them in 2020.

3.International Variations: Online payment methods vary across countries and regions. In Europe and Asia, debit and credit cards are popular, while some countries prefer invoicing and mobile bank transfers. Specific payment systems like iDEAL in the Netherlands and Alipay in China are widely used. There are several international payment gateways available in India, including Cashfree, PayU, Razorpay, and Paytm.

4.Online Credit Card Transactions: Online credit card transactions are similar to in-store purchases but have some differences. These transactions are referred to as "Card Not Present" (CNP) transactions. The lack of physical presence and signatures can lead to disputes and chargebacks.

5. **Payment Enablers**: Online payment service providers, such as Authorize.net, help merchants set up accounts and process credit card payments. These providers offer software tools for online transactions. Payment enablers in India include the Reserve Bank of India (RBI), the Digital India program, and Unified Payments Interface (UPI).
6. **PCI-DSS Compliance**: Payment Card Industry-Data Security Standard (PCI-DSS) is a global data security standard required for accepting credit card payments online. Non-compliance may result in fines and security breaches.
7. **Limitations of Credit Card Payments**: Credit card payments have limitations related to security, high administrative and transaction costs, and accessibility for individuals without credit cards.
8. **Alternative Online Payment Systems**: PayPal, Amazon Pay, WhatsApp Pay, Facebook Pay, Visa Checkout, MasterPass, and other alternatives have emerged to address the limitations of credit card payments. PayPal is one of the most widely used online payment systems.

- **Mobile Payment Systems**: Mobile payments, facilitated by mobile wallet apps, are the fastest-growing alternative payment method. There are three primary types of mobile wallet apps: universal proximity wallets, branded store proximity wallets, and P2P apps.

  - **Universal proximity mobile wallets**, such as Apple Pay, Google Pay, and Samsung Pay, that can be used at a variety of merchants for point-of-sale transactions if the merchant supports that service (e.g., has an Apple merchant app and can accept such payments), are the most-well known and common type.
  - Paytm, Freecharge, Mobikwik, Oxigen, mRuppee, Airtel Money, Jio Money, SBI Buddy, itz Cash, Citrus Pay, Vodafone M-Pesa, Axis Bank Lime, ICICI Pockets, SpeedPay etc.
  - **Branded store proximity mobile wallets** are mobile apps that can be used only at a single merchant. For instance, Walmart, Tesco, and Starbucks all have very successful mobile wallet apps.
  - **P2P mobile payment apps**, such as PayPal, Samsung Pay, Apple Pay, Venmo and Square Cash, are used for payments among individuals who have the same app.

- **Blockchain and Cryptocurrencies**: Blockchain is a decentralized technology that enables secure and transparent transactions. Bitcoin is a prominent example of a cryptocurrency using blockchain. Bitcoin has gained acceptance in the financial world but is also known for its price volatility and security issues. Bitcoin present value 80,94,876.63INR
- **Altcoins**: Apart from Bitcoin, there are many other cryptocurrencies known as "altcoins." These cryptocurrencies aim to improve upon the Bitcoin model or serve different purposes.
- **Initial Coin Offerings (ICOs)**: Some startups raise capital through ICOs, issuing cryptocurrency tokens that can be used to purchase goods and services from the company. However, ICOs have faced regulatory challenges.

Electronic payment systems

E-commerce sites use electronic payment, where electronic payment refers to paperless monetary transactions. Electronic payment has revolutionized the business processing by reducing the paperwork, transaction costs, and labor cost. Being user friendly and less time-consuming than manual processing, it helps business organization to expand its market reach/expansion.

Listed below are some of the modes of electronic payments −

- Credit Card
- Debit Card
- Smart Card
- E-Money
- Electronic Fund Transfer (EFT)

Smart cards

- Smart card is again similar to a credit card or a debit card in appearance, but it has a small microprocessor chip embedded in it. It has the capacity to store a customer’s work-related and/or personal information. Smart cards are also used to store money and the amount gets deducted after every transaction.
- Smart cards can only be accessed using a PIN that every customer is assigned with. Smart cards are secure, as they store information in encrypted format and are less expensive/provides faster processing. Mondex and Visa Cash cards are examples of smart cards.
- Smart cards are basically two types : Relationship based smart card and electronic purses

Relationship based smart card

- Provides enhancement to existing card services it includes access to multiple financial accounts, value added marketing program and other information that card holder want to store on their card
- It offers consumer greater options including the following:

1. Access to multiple account e.g. debit, credit, investment of stored value for e cash
2. Variety of options like cash access, bill payment, balance enquiry and fund transfer for selected accounts
3. Multiple access option using multiple device types such as ATM, phone , personal computer, personal digital assistant.

Electronic purses

- Wallet- sized smart card embedded with programmable microchip that store sum of money for people to use instead of cash for everything for buying food and services.
- Example is paytm wallet
- The electronic purse works in the following manner:

1. After purse is loaded with money at an ATM, it can be used to pay for candy in a vending machine with a card reader.
2. It verifies card is authenticated & it has enough money, the value is deducted from balance on the card & added to an e-cash & remaining balance is displayed by the vending machine.

Credit Card

Payment using credit card is one of most common mode of electronic payment. Credit card is small plastic card with a unique number attached with an account. It has also a magnetic strip embedded in it which is used to read credit card via card readers. When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle.

Following are the actors in the credit card system.

- The card holder − Customer
- The merchant − seller of product who can accept credit card payments.
- The card issuer bank − card holder's bank
- The acquirer bank − the merchant's bank
- The card brand − for example , visa or Mastercard.

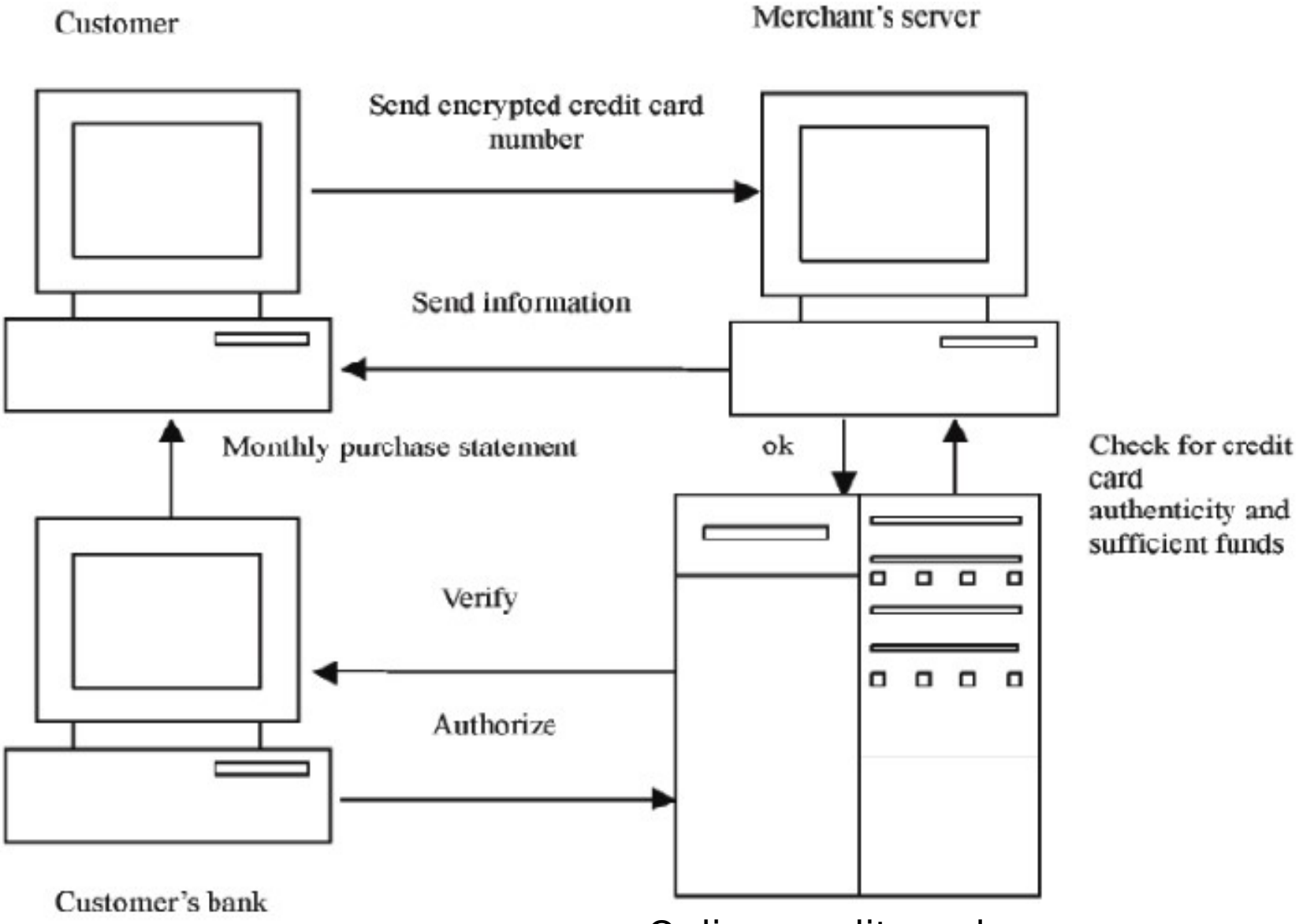
- Credit card payment can be done using three categories:

1. Payment using plain card details
2. Payment using encrypted card details
3. Payment using third party verification

Encryption and credit card

The following sequence of steps must occur before actual goods, services, or funds flow:

- A customer presents his or her credit card information (along with an authenticity signature or other information such as mother’s maiden name) securely to the merchant.
- The merchant validates the customer’s identity as the owner of the credit card account.
- The merchant relays the credit card charge information and signature to its bank or on-line credit card processors.
- The bank or processing party relays the information tot the customer’s; bank for authorization approval.
- The customer’s bank returns the credit card data, charge authentication, and authorization to the merchant.



Online credit card processor

Credit Card Payment Process

Step	Description
Step 1	Bank issues and activates a credit card to the customer on his/her request.
Step 2	The customer presents the credit card information to the merchant site or to the merchant from whom he/she wants to purchase a product/service.
Step 3	Merchant validates the customer's identity by asking for approval from the card brand company.
Step 4	Card brand company authenticates the credit card and pays the transaction by credit. Merchant keeps the sales slip.
Step 5	Merchant submits the sales slip to acquirer banks and gets the service charges paid to him/her.
Step 6	Acquirer bank requests the card brand company to clear the credit amount and gets the payment.
Step 7	Now the card brand company asks to clear the amount from the issuer bank and the amount gets transferred to the card brand company.

How Credit Card Processing Works:

- Let’s take a look at each of the key players involved in authorizing and settling a credit card transaction, and then we’ll move on to examine each process individually in more detail. The key players involved in authorization and settlement are the cardholder, the merchant (business), the acquiring bank (the merchant’s bank), the issuing bank (the cardholder’s bank), and the card associations (Visa and MasterCard.)

Cardholder

- If you have a credit or debit card (as most of us do), you’re already familiar with the role of the cardholder. But just to be thorough — a cardholder is someone who obtains a bankcard (credit or debit) from a card issuing bank. They then present that card to merchants as payment for goods or services.

Merchant

- Technically, a merchant is any business that sells goods or services. But, only merchants that accept cards as a form of payment are pertinent to our explanation. So with that said, a merchant is any business that maintains a merchant account that enables them to accept credit or debit cards as payment from customers (cardholders) for goods or services provided.

Acquiring Bank (Merchant's Bank)

- An acquiring bank is a registered member of the card associations (Visa and MasterCard). An acquiring bank is often referred to as a merchant bank because they contract with merchants to create and maintain accounts (called merchant accounts) that allow the business to accept credit and debit cards. Acquiring banks provide merchants with equipment and software to accept cards and handle customer service and other necessary aspects involved in card acceptance. The acquiring bank also deposits funds from credit card sales into a merchant's account.

- Interestingly enough, many merchants don't recognize their acquiring bank as the primary provider of their merchant account. Acquiring banks are playing an increasingly hands-off role as the bankcard system evolves. Acquiring banks often enlist the help of third-party independent sales organizations (ISO) and membership service providers (MSP) to conduct and monitor the day-to-day activities of their merchant accounts.

Issuing Bank (Cardholder Bank)

As you've probably guessed, an issuing bank issues credit cards to consumers. The issuing bank is also a member of the card associations (Visa and MasterCard).

Issuing banks pay acquiring banks for purchases that their cardholders make. It is then the cardholder's responsibility to repay their issuing bank under the terms of their credit card agreement.

Card Associations (Visa and MasterCard)

Visa and MasterCard aren't banks and they don't issue credit cards or merchant accounts. Instead, they act as a custodian and clearing house for their respective card brand. They also function as the governing body of a community of financial institutions, ISOs and MSPs that work together in association to support credit card processing and electronic payments. Hence the name, "card associations."

The primary responsibilities of the Card Association are to govern the members of their associations, including interchange fees and qualification guidelines, act as the arbiter between issuing and acquiring banks, maintain and improve the card network and their brand, and, of course, make a profit. That last one has become even more important now that Visa and MasterCard are public companies.

Visa uses their VisaNet network to transmit data between association members, and MasterCard uses their Banknet network.

Third party processors and credit card

- Third party is company that gathers and verifies the payment of funds that flow from one party to another. The buyer need to register itself with the third party company.
- Steps involved Online Credit Card Payment through Online Third Party Processor(OTTP)….

1. After filling all the fields of registration form accurately, Online Third Party Processor account number is given to buyer that relays to the processor, information about buyers profile who uses a credit card as their financial device.
2. The buyer sends a request to seller regarding the online purchase by specifying Online Third Party Processor(OTTP) account number. There are two ways in which the purchase request is made.
   - The buyer gives the access privileges to seller who can access his/her account number and produces the bill.
   - The buyer himself can enter the account details.
   3. The seller then submit the buyers account number to Online Third Party Processor(OTTP) accounting server to make an Online Credit Card Payment.

4. Accounting server after receiving the account details verifies if the account number specifies is accurate and does the account have sufficient amount for making an online credit card payment.
5. The accounting server then sends an email or any electronic message to the buyer who can make the acceptance/reject it.
6. If Online Third Party Processor(OTTP) server receives positive acknowledgement, a message is send to the seller who then allow the buyer to access the resources if its an online product.
7. OTTP Server will store the buyer's account details unless it receives the acknowledgement about the completion of the purchase process.

Online Payment Process

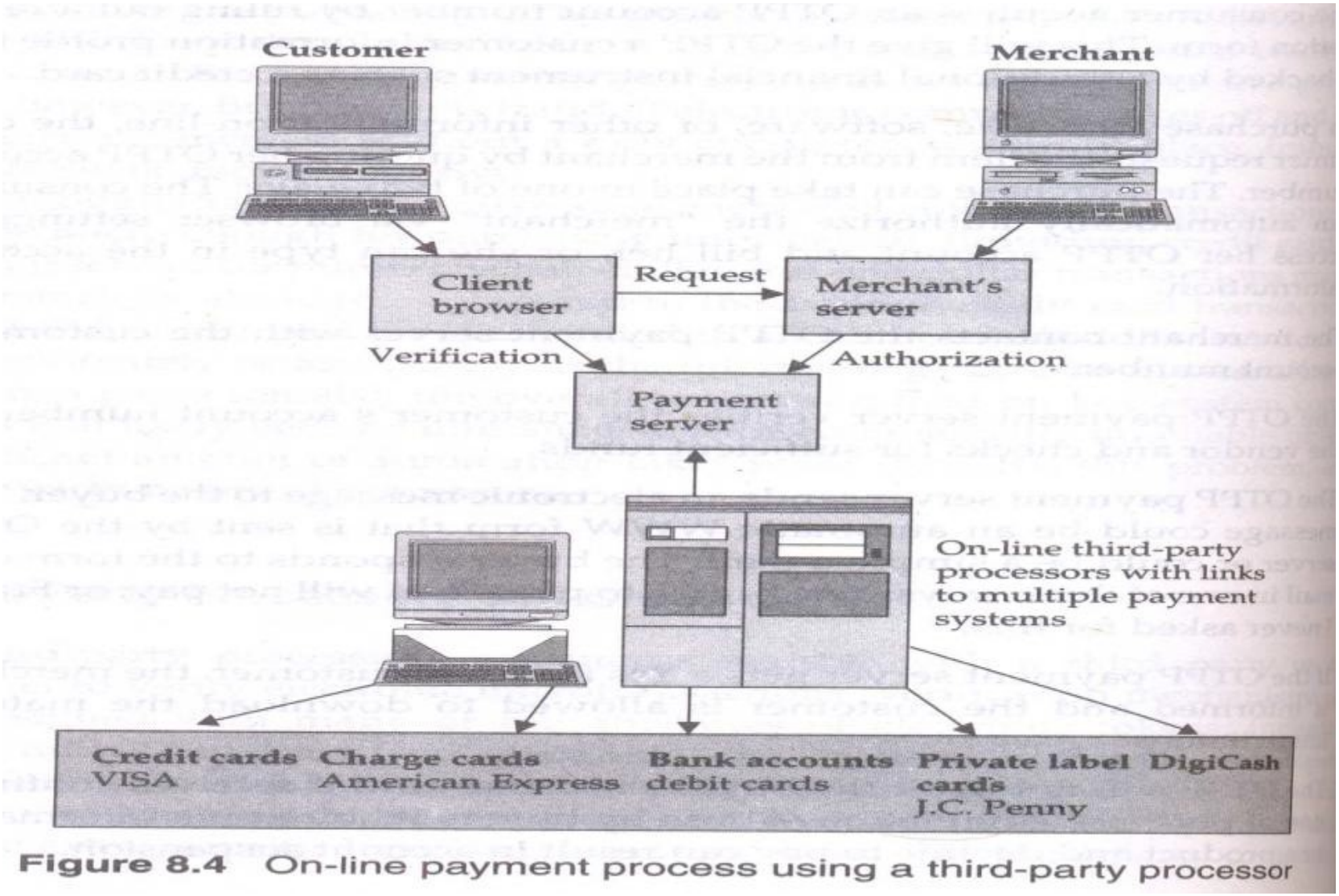


Figure 8.4 On-line payment process using a third-party processor

Debit Card

Debit card, like credit card, is a small plastic card with a unique number mapped with the bank account number. It is required to have a bank account before getting a debit card from the bank.

The major difference between a debit card and a credit card is that in case of payment through debit card, the amount gets deducted from the card's bank account immediately and there should be sufficient balance in the bank account for the transaction to get completed; whereas in case of a credit card transaction, there is no such compulsion.

Debit cards free the customer to carry cash and cheques.

Even merchants accept a debit card readily.

Having a restriction on the amount that can be withdrawn in a day using a debit card helps the customer to keep a check on his/her spending.

Contact smart cards

Contact smart cards have a contact area of approximately 1 square centimeter (0.16 sq in), comprising several gold-plated contact pads. These pads provide electrical connectivity when inserted into a reader, which is used as a communications medium between the smart card and a host (e.g., a computer, a point of sale terminal) or a mobile telephone. Cards do not contain batteries; power is supplied by the card reader

Contactless smart cards

A second card type is the contactless smart card, in which the card communicates with and is powered by the reader through RF induction technology. These cards require only proximity to an antenna to communicate. Like smart cards with contacts, contactless cards do not have an internal power source. Instead, they use an inductor 'to capture some of the incident radio-frequency interrogation signal, rectify it, and use it to power the card's electronics

Example of widely used contactless smart cards are London's Oyster card, Hong Kong's Octopus card, Tokyo's Suica and Pasmo cards used for public transportation

E-Money

E-Money transactions refer to situation where payment is done over the network and the amount gets transferred from one financial body to another financial body without any involvement of a middleman.

E-money transactions are faster, convenient, and saves a lot of time.

Online payments done via credit cards, debit cards, or smart cards are examples of e-money transactions.

Another popular example is e-cash.

In case of e-cash, both customer and merchant have

Electronic Fund Transfer

It is a very popular electronic payment method to transfer money from one bank account to another bank account. Accounts can be in the same bank or different banks.

Fund transfer can be done using ATM (Automated Teller Machine) or using a computer.

Nowadays, internet-based EFT is getting popular. In this case, a customer uses the website provided by the bank, logs in to the bank's website and registers another bank account. He/she then places a request to transfer certain amount to that account.

Customer's bank transfers the amount to other account if it is in the same bank, otherwise the transfer request is forwarded to an ACH (Automated Clearing House) to transfer the amount to other account and the amount is deducted from the customer's account.

Once the amount is transferred to other account, the customer is notified of the fund transfer by the bank.

Designing Electronic Payment systems

It includes several factors:

• Privacy. A user expects to trust in a secure system; just as a telephone is a safe

• Security. A secure system verifies the identity of two-party transactions through —user authentication‖ & reserves flexibility to restrict information/services through access control

• Intuitive interfaces. The payment interface must be as easy to use as a telephone.

• Database integration. With home banking, for ex, a customer wants to play with all his accounts.

• Brokers. A —network banker‖-someone to broker goods & services, settle conflicts, & financial transactions electronically-must be in place

• Pricing. One fundamental issue is how to price payment system services. For e.g., from cash to bank payments, from paper-based to e-cash. The problem is potential waste of resources.

• Standards. Without standards, the welding of different payment users into different networks & different systems is impossible.

Risks in Electronic Payment systems

- Operation on payment system has three major risks: fraud or mistake, privacy issues, credit risk.
- Risk form mistake and dispute:
- consumer protection :Virtually all electronic payment systems require some ability to keep automatic records. Once information has been electronically caught , it is easy and less expensive to keep.
- The intangible nature of electronic transactions and resolution of the disputes relying alone on records, a general law of payment dynamics and banking technology might be : No data should be discarded.

- Features of these automatic records are :
- Permanent storage
- Accessibility and traceability
- A payment system database and
- Data transfer to payment maker, bank or monetary authorities.

The need of keeping of records for the purposes of risk management conflicts with the transaction anonymity of cash. An unknown payment system without automatic record keeping facility will be difficult for bankers and government to accept. However, customers might feel that all this record keeping is an invasion of privacy.

- Managing Information Privacy: Privacy must be maintained against eavesdroppers on the network and against unauthorized insiders. The users must be given assurance that they cannot be easily duped or falsely implicated in a fraudulent transaction. This protection has to be applied on the whole transaction protocol.

- Managing Credit Risk: Credit risk is an important concern in systems of net settlement because a bank’s inability to settle its net position could give rise to a chain reaction of failures of the banks. The digital central bank must prepare policies to handle this possibility.